

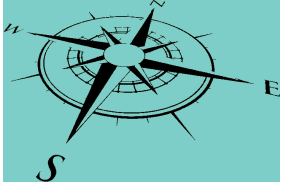
Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense -- Responsibilities of the DoD CIO

Contents

- Mission.....3
- a. Enterprise Governance4
- b. IT Standards5
- c. Data Framework6
- d. NIEM Governance7
- e. Metrics.....8
- f. Acquisition Oversight9
- g. Information Sharing10
- h. Exceptions.....11
- i. Information Sharing Standards.....12
- j. Security Classification13
- k. IT Services14
- l. Shared Services15
- m. Classification, Storage & Handling.....16
- n. Data Sharing.....17
- o. Data Protection.....18
- p. Education & Training.....19
- q. NIEM Compliance20
- r. Compliance & Enforcement21
- s. COIs.....22
- t. Protection23

DEMONSTRATION ONLY

DEMONSTRATION ONLY



U.S. Department of Defense (DOD)

Mission

To document the responsibilities of the DoD CIO

DEMONSTRATION ONLY

a. Enterprise Governance

Establish and oversee the DoD enterprise governance processes for the sharing of data, information, and IT services

Establishes and oversees the DoD enterprise governance processes for the sharing of data, information, and IT services, to include the coordination and adjudication of issues across IT investment portfolios, authoritative bodies (ABs), mission areas, and COIs, in accordance with References (b), (d), DoDD 8115.01 (Reference (x)), and the DoD CIO Executive Board (EB) governance structure.

DEMONSTRATION ONLY

b. IT Standards

Establish policy, assign responsibilities, and provide direction for identifying, developing, and prescribing DoD standards for information technology (IT) systems.

Establishes policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for information technology (IT) systems that enable the use of enterprise capabilities to guide DoD Components in realizing the DoD IE end state described in Reference (f).

DEMONSTRATION ONLY

c. Data Framework

Develop and mature a DoD data framework.

Develops and matures a DoD data framework that provides guidance regarding exchanges of data, their structure, and roles of information exchange models such as NIEM adoption across the DoD.

DEMONSTRATION ONLY

d. NIEM Governance

Coordinate the DoD representation to the NIEM Federal Governance Structure.

Coordinates the DoD representation to the NIEM Federal Governance Structure, including consolidating DoD requirements and position regarding the evolution of NIEM.

DEMONSTRATION ONLY

e. Metrics

Develops metrics for measuring progress in achieving the DoD goals for sharing data, information, and IT services.

Stakeholder(s)

Deputy Chief Management Officer (DCMO)

Under Secretary of Defense for Intelligence (USD(I))

CJCS

Develops metrics, in collaboration with the Deputy Chief Management Officer (DCMO), CJCS, and the Under Secretary of Defense for Intelligence (USD(I)), and select DoD Components for measuring progress in achieving the DoD goals for sharing data, information, and IT services. Metrics developed must meet testable technical requirements (i.e., visible, accessible, understandable, trusted or secure, and interoperable), in accordance with DoD CIO Memorandum (Reference (y)) and DoD Chief Information Memorandum (Reference (z)), and be published to the DoD Components.

f. Acquisition Oversight

Provide acquisition oversight for data, information, and IT services-sharing capabilities.

Stakeholder(s)

Under Secretary of Defense for Acquisition,
Technology, and Logistics (USD(AT&L))

Provides acquisition oversight for data, information, and IT services-sharing capabilities when designated as the Milestone Decision Authority by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) in accordance with Reference (m) and DoDD 5000.01 (Reference (aa)).

DEMONSTRATION ONLY

g. Information Sharing

Address information-sharing requirements of the Combatant Commands.

Stakeholder(s)

CJCS

Combatant Commands

Coordinates with the CJCS in addressing information-sharing requirements of the Combatant Commands.

DEMONSTRATION ONLY

h. Exceptions

Adjudicate DoD Component requests for exceptions.

Adjudicates DoD Component requests for exceptions to compliance with this instruction and the use of enterprise services, interface specifications, and standards for the exchange of DoD data and information.

DEMONSTRATION ONLY

i. Information Sharing Standards

Direct the development and distribution of a core set of standards for electronic information sharing.

Stakeholder(s)

Under Secretary of Defense for Policy (USD(P))

CJCS

Directs, for unclassified information sharing capabilities, the development and distribution of a core set of standards for electronic information sharing, including associated applications. These are developed in coordination with the Under Secretary of Defense for Policy (USD(P)) and CJCS, in accordance with DoDI 8110.01 (Reference (ab)).

DEMONSTRATION ONLY

j. Security Classification

Issue a security classification guide.

Stakeholder(s)

USD(P)

Chief, Central Security Service (DIRNSA/CHCSS)

Director, National Security Agency

USD(I)

Issues a security classification guide regarding information sharing capability (e.g., software, hardware, architectures, configurations) in coordination with the USD(P), Director, National Security Agency/ Chief, Central Security Service (DIRNSA/CHCSS), and USD(I) and in accordance with Volume 1 of DoDM 5200.01 (Reference (ac)).

DEMONSTRATION ONLY

k. IT Services

Evaluate candidate IT services.

Evaluates candidate IT services submitted by the DoD Components for enterprise reuse and potential designation as an enterprise service.

DEMONSTRATION ONLY

I. Shared Services

Track and evaluate data, information, and IT services-sharing capabilities.

Tracks and evaluates data, information, and IT services-sharing capabilities provided to the DoD Components.

DEMONSTRATION ONLY

m. Classification, Storage & Handling

Develop guidance for data classification caveats, storage, handling, and distribution requirements and tagging, discovery, and access to data.

Stakeholder(s)

USD(I)

Intelligence Community (IC)

Aids the USD(I), in coordination with the Intelligence Community (IC), to develop standardized guidance for use with other federal agencies with regard to data classification caveats, storage, handling, and distribution requirements and tagging, discovery, and access to data.

DEMONSTRATION ONLY

n. Data Sharing

Guide and oversee data sharing.

Stakeholder(s)

DoD Components

COIs

Guides and oversees matters relating to data sharing in support of the DoD Components, COIs, and IT portfolios, in accordance with Reference (a), by supporting, influencing, and enforcing enterprise metadata direction that uses existing government and industry metadata standards.

DEMONSTRATION ONLY

o. Data Protection

Develop policies and procedures to protect data.

Stakeholder(s)

| | |
|-------------------|--------------|
| Mission Partners | USD(P) |
| Federal Agencies | DNI |
| State Governments | DIRNSA/CHCSS |
| Local Governments | CJCS |
| USD(I) | |

Develops the policies and procedures to protect data while enabling data sharing across security domains and with mission partners, other federal agencies, and State and local governments, in coordination with the USD(I), USD(P), DNI, DIRNSA/CHCSS, and CJCS, in accordance with applicable laws, DoD policy, and security classifications.

DEMONSTRATION ONLY

p. Education & Training

Ensures that data, information, and IT services-sharing concepts and practices are incorporated into education and awareness training.

Stakeholder(s)

| | |
|--------------------------------|-----------|
| National Defense University | CJCS |
| Defense Acquisition University | USD(AT&L) |
| Military Service Schools | USD(P&R) |

Develops and ensures that data, information, and IT services-sharing concepts and practices are incorporated into education and awareness training through the National Defense University, Defense Acquisition University, Military Service schools, and appropriate DoD processes in coordination with the CJCS, USD(AT&L), and USD(P&R).

DEMONSTRATION ONLY

q. NIEM Compliance

Establish and maintain the processes and governance to ensure compliance with the “Consider NIEM First” policy.

Establishes and maintains the processes and governance to ensure compliance with the “Consider NIEM First” policy. Clarifies how NIEM relates to the use of the core set of standards and shared vocabularies for information exchange and applications developed, in accordance with Reference (d), DoD Discovery Metadata Specification (DDMS) (Reference (ad)), and DISR-approved standards and specifications.

DEMONSTRATION ONLY

r. Compliance & Enforcement

Define policy and oversight for compliance and enforcement of this instruction.

Defines policy and oversight for a “tiered accountability” approach for compliance and enforcement of this instruction.

DEMONSTRATION ONLY

s. COIs

Provide oversight to COIs aligned to the Enterprise Information Environment Mission Area.

Provides governance oversight to those COIs aligned to the Enterprise Information Environment Mission Area.

DEMONSTRATION ONLY

t. Protection

Develop policies, procedures, standards, and standards frameworks to protect data, information, and IT services.

Stakeholder(s)

USD(P)

IC CIO

USD(I)

DoD Component Heads

Collaborates with the USD(P), USD(I), IC CIO, and DoD Component heads in developing policies, procedures, standards, and standards frameworks to protect data, information, and IT services while enabling their secure sharing as strategic assets, in accordance with this instruction, Reference (ac), and Intelligence Community Directive (ICD) 501 (Reference (ae)), ICD 502 (Reference (af)), and ICD 503 (Reference (ag)).

DEMONSTRATION ONLY